OneLook® Dictionary Search

Home About Browse Dictionaries Customize

**Word or phrase:** symmetric key Search

● Find definitions ○ Find translations ○ Search all dictionaries

Jump to: General, Art, Business, Computing, Medicine, Miscellaneous, Religion, Science, Slang, Sports, Tech, Phrases

**We found one dictionary with English definitions that includes the word *symmetric key*:**
*Tip: Click on the first link on a line below to go directly to a page where "symmetric key" is defined.*

➾ **General** (1 matching dictionary)

1. Symmetric key : Wikipedia, the Free Encyclopedia [home, info]

Encyclopedia article (***Symmetric key algorithm***)

A **symmetric-key algorithm** is an algorithm for cryptography that uses the same cryptographic key to encrypt and decrypt the message. (Actually, it is sufficient for it to be easy to compute the decryption key from the encryption key and vice versa.) Other terms for symmetric-key encryption are *single-key* and *private-key* encryption. (continued at Wikipedia)

Phrases that include ***symmetric key***: symmetric key cryptography, symmetric key algorithm

Additional searches for *symmetric key...*

*Search completed in 0.504 seconds.*

OneLook® Dictionary Search

Home About Browse Dictionaries Customize Link to us Reverse Dictionary Word of the Day

□‹□Œù“I□□ÇÚä¡ÿ´-□&™¶W”Ðod› ÆT§□ÔbGuì®□□-C□eUw□î□uC
□ÑjÔ?ä ÿ˜}Pa™{S□□1›«□ÊDG °§hbuQ» z\e□ó[â¼ □áxÖ+ø□□†ƒ
”ÏZ9□□(Þ¾|F‡Qü□□¾ñ□C…i²G+s×#G*»³…%ýàá½`k7Û□èÃ¿ î’iöå“3keV□□»t|µÊ%□ÜtÑ
JåÑ□□ªéü{□•ø\V□»›QQ‹96ÛÄ<3óÒitÃrªä□Ì¾|ü□Ü~ªäÍR□ÍÑ□□□í_5Rü□#ÚWI□.Ù±P«dóÆÆ□ç?·
□02qÈÙ±Ñ9í_õêl èƒBï[é¢u!Yñ»P°Œ[ô™ÿþ¬uJ□œŒ.&ñÂ«IgCŸzŸÐRD±™Ù§{□‹□LÜ
‹ˆ@ÜoÒkxqW»Y□‹“Æ“ì¦□Óž•Ö□Æ□ù·ƒO°ñ~Ì□vM6—□[Í□8oÁR)¥2üf□ri-b§KwN□W‰‚›□□J□lj«
÷J¸ÆÆ ·Kh□¤Çˆ L8Wsd□¹iéÊ□îW#™ˆ*@bÖ□g*q˜□ÝÔãy„□#Z2R×Bïu5Êê–•ì□5□Ã›h
#.·o°S»‹Ly»=?,%È ø eC¥¾□Ãi›ƒ¦3RäÃD•Ó□□C€£□.¶ÍÇ0XzG¬□ÿ6ÓÉåí´=Ø’ô¨ñä)wi□¹]F2»…Ï[
×Ö‘ŒÓƒ$d™T´BÎVR-SØ□□Ïñ•µ¿çK—[¥©□ó?`næ‹[Ë¹ãeqÂàÄó□7□k$£˜□É?□/|ˆpk·nLB¦ŸFÄ-„ùR□
Zÿ?{□ìÙ{ó°êãïuo¾n:□¡[íuß□ cÿµz·²□þ¯xoLÿã—\ìznF¾½q±´N8ÛŽë&Ìuk†Î
…□å□Ã…B□ö¿9ºÿà€ú÷è¥0„¹öA—N³Œ¼fñ>-íS½ï½yÇbûd□ïËþ
S¥¿ç…AV¿C³□…ë’T:èjïv?„îõKëöõÛç□□è%
[µÓ3iêsÌ)={óøÉ ½x¥¹¬□□ÇúDB²‰ì□Òõê`¥F□ˆ_2$“>é□Æ<û‘.1×□Ôen5¤n_K¥xæÑ□_8L□□]t□DÑŽ
úÛ²□ý□£›ËÚÔ,oýä§}uµ-dþjEh'3 î:/wk±□8□¿—ãÑ,ÇŽð=«ŒaÉpB(|B¬=û˜ýö
N°û'WžóýÂœˆkã8¦6WV,mzò÷;üÞþîç7□□÷x%õ_□€÷□Eö›ŒÀû‹÷›□ÁÛ□d{µ¨¿}›ßC„5ð,~ò!uc]j¦7:pâ†C
/gÄ±Æˆá;½□šÇx2˜k□÷…À6Z°EjèÂƒ6èÖÏéóN‡.@‘/>“p …Ièˆ□»ýC¾á±]êt‚‰ñ□Ý

First Hit Fwd Refs
End of Result Set

□ Generate Collection Print

L4: Entry 1 of 1 File: USPT Jun 3, 2003

DOCUMENT-IDENTIFIER: US 6574609 B1
TITLE: Secure electronic content management system

Detailed Description Text (58):
Symmetric key algorithms are much faster than the public key algorithms. In software, DES is generally at least 100 times as fast as RSA. Because of this, RSA is not used to encrypt bulk data. RSA Data Security reports that on a 90 MHZ Pentium machine, RSA Data Security's toolkit BSAFE 3.0 has a throughput for private-key operations (encryption or decryption, using the private key) of 21.6 kilobits/second with a 512-bit modulus and 7.4 kilobits/second with a 1024-bit modulus.

Detailed Description Text (60):
In the Secure Digital Content Electronic Distribution System 100, the issuer of SC (s) protects the integrity of SC(s) by digitally signing it. In general, to create a digital signature of a message, a message owner first computes the message digest (defined below) and then encrypt the message digest using the owner's private key. The message is distributed with its signature. Any recipient of the message can verify the digital signature first by decrypting the signature using the public key of the message owner to recover the message digest. Then, the recipient computes the digest of the received message and compare it with the recovered one. If the message has not being altered during distribution, the calculated digest and recovered digest must be equal.

Detailed Description Text (61):
In the Secure Digital Content Electronic Distribution System 100, since SC(s) contain several data parts, a digest is calculated for each part and a summary digest is calculated for the concatenated part digests. The summary digest is encrypted using the private key of the issuer of the SC(s). The encrypted summary digest is the issuer's digital signature for the SC(s). The part digests and the digital signature are included in the body of the SC(s). The recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests.

Detailed Description Text (115):
SC(s) include at least one bill of materials (BOM) part which has records of information about the SC(s) and about each of the parts included in the SC(s). A message digest is calculated, using a hashing algorithm such as MD-5, for each part and then included in the BOM record for the part. The digests of the parts are concatenated together and another digest is computed from them and then encrypted using the private key of the entity creating the SC(s) to create a digital signature. Parties receiving the SC(s) can use the digital signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts.

Detailed Description Text (181):
One Symmetric Key 623 is used for decrypting the watermarking instructions and the other for decrypting the Content 113 and any encrypted metadata. The watermarking

instructions are included within the Metadata SC(s) 620 portion in the Order SC(s) 650. The Content 113 and encrypted metadata are in the Content SC(s) 630 at a Content Hosting Site(s) 111. The URL and part names of the encrypted Content 113 and metadata parts, within the Content SC(s) 630, are included in the Key Description part of the Metadata SC(s) 620 portion of the Order SC(s) 650. The Clearinghouse(s) 105 uses its private key to decrypt the Symmetric Keys 623 and then encrypts each of them using the Public Key 661 of the End-User Device(s) 109. The Public Key 661 of the End-User Device(s) 109 is retrieved from the Order SC(s) 650. The new encrypted Symmetric Keys 623 is included in the Key Description part of the License SC(s) 660 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109.

Detailed Description Paragraph Table (3):
Step Process 301 Sender generates a random symmetric key and uses it to encrypt the content. 302 Sender runs the encrypted content through a hash algorithm to produce the content digest. 303 Sender encrypts the symmetric key using the recipient's public key. PB RECPNT refers to the recipient's public key. 304 Sender runs the encrypted symmetric key through the same hash algorithm used in step 2 to produce the symmetric key digest. 305 Sender runs the concatenation of the content digest and symmetric key digest through the same hash algorithm used in step 2 to produce the SC(s) digest. 306 Sender encrypts the SC(s) digest with the sender's private key to produce the digital signature for the SC(s). PV SENDER refers to the sender's private key. 307B Sender creates a SC(s) file that includes the encrypted content, encrypted symmetric key, content digest, symmetric key digest, sender's certificate, and SC(s) signature. 307A Sender must have obtained the certificate from a certification authority prior to initiating secure communications. The certification authority includes in the certificate the sender's public key, the sender's name and signs it. PV CAUTHR refers to the certifications authority's private key. Sender transmits the SC(s) to the recipient.

First Hit Fwd Refs
End of Result Set

□ Generate Collection Print

L6: Entry 1 of 1 File: USPT Jun 3, 2003

DOCUMENT-IDENTIFIER: US 6574609 B1
TITLE: Secure electronic content management system

Detailed Description Text (130):
The Clearinghouse(s) 105 validates and processes Order SC(s) 650 to provide the End-User Device(s) 109 with everything that is required to a License Watermark 527 and access purchased Content 113. One of the functions of the Clearinghouse(s) 105 is to decrypt the Symmetric Keys 623 that are needed to decrypt the watermarking instructions from the Offer SC(s) 641 and the Content 113 from the Content SC(s) 630. An encrypted Symmetric Key 623 record actually contains more than the actual encrypted Symmetric Key 623. Before executing the encryption, the Content Provider (s) 101 appends its name to the actual Symmetric Key 623. Having the Content Provider(s)' 101 name encrypted together with the Symmetric Key 623 provides security against a pirate Content Provider(s) 101 that has built its own Metadata SC(s) 620 and Content SC(s) 630 from legal SC(s). The Clearinghouse(s) 105 verifies that the name of the Content Provider(s) 101 encrypted together with the Symmetric Keys 623 matches the name of the Content Provider(s) 101 in the SC(s) certificate.

Detailed Description Text (143):
The following describes the terms that are used in the above Transaction SC(s) 640 that were not previously described for another SC(s): Transaction ID 535--An ID assigned by the Electronic Digital Content Store(s) 103 to uniquely identify the transaction. End-User(s) ID--An identification of the End-User(s) obtained by the Electronic Digital Content Store(s) 103 at the time the End-User(s) makes the buying selection and provides the credit card information. End-User(s)' Public Key--The End-User(s)' Public Key 661 that is used by the Clearinghouse(s) 105 to re-encrypt the Symmetric Keys 623. The End-User(s)' Public Key 661 is transmitted to the Electronic Digital Content Store(s) 103 during the purchase transaction. Offer SC(s)--Offer SC(s) 641 for the Content 113 items that were purchased. The Offer SC (s) do not have digests computed because each container can be validated individually. Offer SC(s) BOMs--BOM parts of the Offer SC(s) 641 that are included as parts in the Transaction SC(s) 640. The Transaction SC(s) 640 BOM has a record for each of the Offer SC(s) 641 BOM parts. The record includes a digest of the BOM part and a parameter that identifies the name of the Offer SC(s) 641 part that is associated with this Offer SC(s) 641 BOM part. After each Offer SC(s) 641 is unpacked by the packer, a digest is computed for its BOM and compared with the digest of its associated Offer SC(s) 641 BOM record in the Transaction SC(s) 640. If the digests match, then the BOMs are identical and the appropriate Offer SC(s) 641 was really included in the Transaction SC(s) 640. If the digest do not match, then the SC(s) is not valid. Selections of Content Use--An array of Usage Conditions for each Content 113 item being purchased by the End-User(s). There is an entry for each Offer SC(s) 641. HTML to Display--One or more HTML pages that the End-User Player Application 195 displays in the Internet browser window upon receipt of the Transaction SC(s) 640 or during the interaction between the End-User Device(s) 109 and the Clearinghouse(s) 105. When the End-User Device(s) 109 receives a Transaction SC(s) 640, the following steps may be performed to verify the integrity and authenticity of the SC(s): 1. Verify the integrity of the Electronic Digital Content Store(s) 103 certificate using the Public Key 621 of the

Clearinghouse(s) 105. The Public Key 621 of the Clearinghouse(s) 105 was stored at the End-User Device(s) 109 after it was received as part of the initialization of the End-User Player Application 195 during its installation process. 2. Verify the Digital Signature 643 of the SC(s) using the public key from the Electronic Digital Content Store(s) 103 certificate. 3. Verify the hashes of the SC(s) parts. 4. Verify the integrity and authenticity of each Offer SC(s) 641 included in the Transaction SC(s) 640. 5. Compute the hashes of BOMs from each Offer SC(s) 641 and compare them against the hashes of the Offer SC(s) 641 BOMs that are included as parts in the Transaction SC(s) 640.

Detailed Description Text (176):
The Clearinghouse(s) 105 begins the validation of Order SC(s) 650 by verifying the digital signatures, then the Clearinghouse(s) 105 verifies the integrity of the Order SC(s) 650 parts. To validate the digital signature, first the Clearinghouse (s) 105 decrypts the Contents 631 of the signature itself using the Public Key 661 of End-User Device(s) 109 included in the Order SC(s) 650. Then, the Clearinghouse (s) 105 calculates the digest of the concatenated part digests of the Order SC(s) 650 and compares it with the digital signature's decrypted Content 113. If the two values match, the digital signature is valid. To verify the integrity of each part, the Clearinghouse(s) 105 computes the digest of the part and compares it to the digest value in the BOM. The Clearinghouse(s) 105 follows the same process to verify the digital signatures and part integrity for the Metadata and Offer SC(s) 641 parts included within the Order SC(s) 650.

Detailed Description Text (257):
Final Quality Assurance Process 813 is an optional step that allows a cross reference check between the associated Metadata and Content SC(s) 630 to verify that they match up correctly and that all information and Content 113 contained therein are correct. Upon completion of Final Quality Assurance Process 813, the jobs are queued for Content Dispersement Process 814. If a problem is found, the job in most cases has to be re-queued to the failing stage. Rework at this stage is much more costly since the product has to go through re-encryption and repacking in addition to the reprocessing required to correct the problem. It is highly recommended that the prior assurance stages be used to assure the quality of the Content 113 and accuracy and completeness of the information.

First Hit Fwd Refs
End of Result Set

□ Generate Collection Print

L3: Entry 1 of 1 File: USPT Jun 3, 2003

DOCUMENT-IDENTIFIER: US 6574609 B1
TITLE: Secure electronic content management system

Brief Summary Text (12):
Further information on the background of protecting digital content can be found from the following three sources. "Music on the Internet and the Intellectual Property Protection Problem" by Jack Lacy, James Snyder, David Maher, of AT&T Labs, Florham, Park, N.J. available online URL http://www.a2bmusic.com/about/papers/musicipp.htm. Cryptographically protected container, called DigiBox, in the article "Securing the Content, Not the Wire for Information Commerce" by Olin Sibert, David Bernstein and David Van Wie, InterTrust Technologies Corp. Sunnyvale, Calif. available online URL http://www.intertrust.com/architecture/stc.html. And "Cryptolope Container Technology", an IBM White Paper, available online URL http:///cyptolope.ibm.com/white.htm.

Drawing Description Text (3):
FIG. 2 is a block diagram illustrating an example Secure Container (SC) and the associated graphical representations according to the present invention.

Drawing Description Text (4):
FIG. 3 is a block diagram illustrating an overview of the encryption process for a Secure Container (SC) according to the present invention.

Drawing Description Text (5):
FIG. 4 is a block diagram illustrating an overview of the de-encryption process for a Secure Container (SC) according to the present invention.

Detailed Description Text (3):
Table of Contents I. SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM A. System Overview 1. Rights Management 2. Metering 3. Open Architecture B. System Functional Elements 1. Content Provider(s) 2. Electronic Digital Content Store(s) 3. Intermediate Market Partners 4. Clearinghouse(s) 5. End-User Device(s) 6. Transmission Infrastructures C. System Uses II. CRYPTOGRAPHY CONCEPTS AND THEIR APPLICATION TO THE SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM A. Symmetric Algorithms B. Public Key Algorithms C. Digital Signature D. Digital Certificates E. Guide to the SC(s) Graphical Representation F. Example of a Secure Container Encryption III. SECURE DIGITAL CONTENT ELECTRTONIC DISTRIBUTION SYSTEM FLOW IV. RIGHTS MANAGEMENT ARCHITECTURE MODEL A. Architecture Layer Functions B. Function Partitioning and Flows 1. Content Formatting Layer 2. Content Usage Control Layer 3. Content Identification Layer 4. License Control Layer C. Content Districution and Licensing Control V. SECURE CONTAINER STRUCTURE A. General Structure B. Rights Management Language Syntax and Semantics C. Overview of Secure Container Flow and Processing D. Metadata Secure Container 620 Format E. Offer Secure Container 641 Format F. Transaction Secure Container 640 Format G. Order Secure Container 650 Format H. License Secure Container 660 Format I. Content Secure Container Format VI. SECURE CONTAINER PACKING AND UNPACKING A. Overview B. Bill of Materials (BOM) Part C. Key Description Part VII. CLEARINGHOUSE(S) A.

Overview B. Rights Management Processing C. Country Specific Parameters D. Audit Logs and Tracking E. Reporting of Results F. Billing and Payment Verification G. Retransmissions VIII. CONTENT PROVIDER A. Overview B. Work Flow Manager 1. Products Awaiting Action/Information Process 2. New Content Request Process 3. Automatic Metadata Acquisition Process 4. Manual Metadata Entry Process 5. Usage Conditions Process 6. Supervised Release Process 7. Metadata SC(s) Creation Process 8. Watermarking Process 9. Preprocessing and Compression Process 10. Content Quality Control Process 11. Encryption Process 12. Content SC(s) Creation Process 13. Final Quality Assurance Process 14. Content Dispersement Process 15. Work Flow Rules C. Metadata Assimilation and Entry Tool 1. Automatic Metadata Acquiaition Tool 2. Manual Metadata Entry Tool 3. Usage Conditions Tool 4. Parts of the Metadata SC(s) 5. Supervised Release Tool D. Content Processing Tool 1. Watermarking Tool 2. Preprocessing and Compression Tool 3. Content Quality Control Tool 4. Encryption Tool E. Content SC(s) Creation Tool F. Final Quality Assurance Tool G. Content Dispersement Tool H. Content Promotions Web Site I. Content Hosting 1. Content Hosting Sites 2. Content Hosting Site(s) 111 provided by the Secure Digital Content Electronic Distribution System IX. ELECTRONIC DIGITAL CONTENT STORE(S) A. Overview--Support for Multiple Electronic Digital Content Store(s) B. Point-to-Point Electronic Digital Content Distribution Service 1. Integration Requirements 2. Content Acquisition Tool 3. Transaction Processing Module 4. Notification Interface Module 5. Account Reconciliation Tool C. Broadcast Electronic Digital Content Distribution Service X. END-USER DEVICE(S) A. Overview B. Application Installation C. Secure Container Processor D. The Player Application 1. Overview 2. End-User Interface Components 3. Copy/Play Management Components 4. Decruyption 1505, Decompression 1506 and Playback Components 5. Data Management 1502 and Library Access Components 6. Inter-application Communication Components 7. Other Miscellaneous Components 8. The Generic Player

Detailed Description Text (6):
The Secure Digital Content Electronic Distribution System is a technical platform that encompasses the technology, specifications, tools, and software needed for the secure delivery and rights management of Digital Content and digital content-related content to an end-user, client device. The End-User Device(s) include PCS, set top boxes (IRDs), and Internet appliances. These devices may copy the content to external media or portable, consumer devices as permitted by the content proprietors. The term Digital Content or simply Content, refers to information and data stored in a digital forniat including: pictures, movies, videos, music, programs, multimedia and games.

Detailed Description Text (11):
Licensing authorization and control are implemented through the use of a Clearinghouse(s) entity and Secure Container (SC) technology. The Clearinghouse(s) provides licensing authorization by enabling intermediate or End-User(s) to unlock content after verification of a successful completion of a licensing transaction. Secure Containers are used to distribute encrypted content and information among the system components. A SC is a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection against unauthorized interception or modification of electronic information and content. It also allows for the verification of the authenticity and integrity of the Digital Content. The advantage of these rights management functions is that the electronic Digital Content distribution infrastructure does not have to be secure or trusted. Therefore transmission over network infrastructures such as the Web and Internet. This is due to the fact that the Content is encrypted within Secure Containers and its storage and distribution are separate from the control of its unlocking and use. Only users who have decryption keys can unlock the encrypted Content, and the Clearinghouse(s) releases decryption keys only for authorized and appropriate usage requests. The Clearinghouse(s) will not clear bogus requests from unknown or unauthorized parties or requests that do not comply with the content's usage conditions as set by the content proprietors. In addition, if the SC is tampered with during its transmission, the software in

the Clearinghouse(s) determines that the Content in a SC is corrupted or falsified and repudiate the transaction.

Detailed Description Text (39):
The End-User Device(s) 109 can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications. These devices may include PCS, set top boxes (IRDs), and Internet appliances. The End-User Player Application 195 could be implemented in software and/or consumer electronics hardware. In addition to performing play, record, and library management functions, the End-User Player Application 195 performs SC processing to enable rights management in the End-User Device(s) 109. The End-User Device(s) 109 manages the download and storage ofthe SCs containing the Digital Content; requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of the End-User Player Application 195 functions in order to process the content's Usage Conditions embedded in the watermark. The terms End-User(s) and End-User Player Application 195 are used throughout this to mean through the use or running-on an End-User Device(s) 109.

Detailed Description Text (48):
License Control in the Secure Digital Content Electronic Distribution System 100 is based on the use of cryptography. This section introduces basic cryptography technologies of the present invention. The use of public key encryption, symmetric key encryption, digital signatures, digital watermarks and digital certificates is known.

Detailed Description Text (54):
B. Public Key Algorithms

Detailed Description Text (55):
In the Secure Digital Content Electronic Distribution System 100, symmetric keys and other small data pieces are encrypted using public keys. Public key algorithms use two keys. The two keys are mathematically related so that data encrypted with one key can only be decrypted with the other key. The owner of the keys keeps one key private (private key) and publicly distributes the second key (public key).

Detailed Description Text (56):
To secure the transmission of a confidential message using a public key algorithm, one must use the recipient's public key to encrypt the message. Only the recipient, who has the associated private key, can decrypt the message. Public key algorithms are also used to generate digital signatures. The private key is used for that purpose. The following section provides information on digital signatures.

Detailed Description Text (57):
The most common used public-key algorithm is the RSA public-key cipher. It has become the de-facto public key standard in the industry. Other algorithms that also work well for encryption and digital signatures are ElGamal and Rabin. RSA is a variable-key length cipher.

Detailed Description Text (58):
Symmetric key algorithms are much faster than the public key algorithms. In software, DES is generally at least 100 times as fast as RSA. Because of this, RSA is not used to encrypt bulk data. RSA Data Security reports that on a 90 MHZ Pentium machine, RSA Data Security's toolkit BSAFE 3.0 has a throughput for private-key operations (encryption or decryption, using the private key) of 21.6 kilobits/second with a 512-bit modulus and 7.4 kilobits/second with a 1024-bit

modulus.

Detailed Description Text (60):
In the Secure Digital Content Electronic Distribution System 100, the issuer of SC (s) protects the integrity of SC(s) by digitally signing it. In general, to create a digital signature of a message, a message owner first computes the message digest (defined below) and then encrypt the message digest using the owner's private key. The message is distributed with its signature. Any recipient of the message can verify the digital signature first by decrypting the signature using the public key of the message owner to recover the message digest. Then, the recipient computes the digest of the received message and compare it with the recovered one. If the message has not being altered during distribution, the calculated digest and recovered digest must be equal.

Detailed Description Text (61):
In the Secure Digital Content Electronic Distribution System 100, since SC(s) contain several data parts, a digest is calculated for each part and a summary digest is calculated for the concatenated part digests. The summary digest is encrypted using the private key of the issuer of the SC(s). The encrypted summary digest is the issuer's digital signature for the SC(s). The part digests and the digital signature are included in the body of the SC(s). The recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests.

Detailed Description Text (65):
A digital certificate is used to authenticate or verify the identity of a person or entity that has sent a digitally signed message. A certificate is a digital document issued by a certification authority that binds a public key to a person or entity. The certificate includes the public key, the name of the person or entity, an expiration date, the namne of the certification authority, and other information. The certificate also contains the digital signature of the certification authority.

Detailed Description Text (66):
When an entity (or person) sends a message signed with its private key and accompanied with its digital certificate, the recipient of the message uses the entity's name from the certificate to decide whether or not to accept the message.

Detailed Description Text (69):
This document uses a drawing to graphically represent SC(s) that shows encrypted parts, non-encrypted parts, the encryption keys, and certificates. Referring now to FIG. 2 is an example drawing of SC(s) 200. The following symbols are used in the SC (s) figures. Key 201 is a public or private key. The teeth of the key e.g. CLRNGH for Clearinghouse indicate the key owner. PB inside the handle indicates that it is a public key thus key 201 is a Clearinghouse public key. PV inside the handle indicates that it is a private key. Diamond shape is an End-User Digital Signature 202. The initials indicate which private key was used to create the signature thus in EU is the End-User(s) digital signature from table below. Symmetric key 203 is used to encrypt content. An encrypted symmetric key object 204 comprising a symmetric key 203 encrypted with a PB of CLRNGH. The key on the top border of the rectangle is the key used in the encryption of the object. The symbol or text inside the rectangle indicates the encrypted object (a symmetric key in this case). Another encrypted object, in this example a Transaction ID encrypted object 205 is shown. And Usage Conditions 206 for content licensing management as described below. The SC(s) 200 comprises Usage Conditions 206, Transaction ID encrypted object 205, an Application ID encrypted object 207, and encrypted symmetric key object 204, all signed with an End-User Digital Signature 202.

cited
106

Detailed Description Text (71):
F. Example of a Secure Container Encryption

Detailed Description Text (95):
As part of the Content Identification Layer 503, the Content Provider(s) 101 also uses a License Watermark 527 to embed data in the Content 113 such as to the content identifier, content owner and other information, such as publication date and geographic distribution region. This watermark is referred to here as the Copyright Watermark 529. Upon reception, the End-User Device(s) 109 watermarks the copy of the Content 113 with the content purchaser's name and the Transaction ID 535 (see the License Control Layer 501 section below), and with other information such as date of license and Usage Conditions 517. This watermark is referred to here as the license watermark. Any copy of Content 113, obtained in an authorized manner or not, and subject to audio processing that preserves the content quality, carries the copyright and license watermarks. The Content Identification Layer 503 deters piracy.

Detailed Description Text (97):
The License Control Layer 501 protects the Content 113 against unauthorized interception and ensures that the Content is only released on an individual basis to an End-User(s) that has properly licensed End-User Device(s) 109 and successfully completes a license purchase transaction with an authorized Electronic Digital Content Store(s) 103. The License Control Layer 501 protects the Content 113 by double Encryption 531. The Content 113 is encrypted using an encryption symmetric key generated by the Content Provider(s) 101, and the symmetric key is encrypted using the public key 621 of the Clearinghouse(s). Only the Clearinghouse (s) 105 can initially recover the symmetric key.

Detailed Description Text (104):
The overall licensing flow starts at the Content Provider(s) 101. The Content Provider(s) 101 encrypts the Content 113 using an encryption symmetric key locally generated, and encrypts the Symmetric Key 623 using the Clearinghouse's 105 public key 621. The Content Provider(s) 101 creates a Content SC(s) 630 around the encrypted Content 113, and a Metadata SC(s) 620 around the encrypted Symmetric Key 623, Store Usage Conditions 519, and other Content 113 associated information. There is one Metadata SC(s) 620 and one Content SC(s) 630 for every Content 113 object. The Metadata SC(s) 620 also carries the Store Usage Conditions 519 associated with the Content Usage Control Layer 505.

Detailed Description Text (106):
After the completion of the Content-purchase transaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 (step 603), the Electronic Digital Content Store(s) 103 creates and transfers to the End-User Device(s) 109 a Transaction SC(s) 640 (step 604). The Transaction SC(s) 640 includes a unique Transaction ID 535, the purchaser's name (i.e. End-User(s)') (not shown), the Public Key 661 of the End-User Device(s) 109, and the Offer SC(s) 641 associated with the purchased Content 113. Transaction Data 642 in FIG. 6 represents both the Transaction ID 535 and the End-User(s) name (not shown). The Transaction Data 642 is encrypted with the Public Key 621 of the Clearinghouse(s) 105. Optionally, the Transaction SC(s) 640 is signed with a Digital Signature 643 of the Electronic Digital Content Store(s) 103.

Detailed Description Text (109):
If the verifications are successful, the Clearinghouse(s) 105 decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the License SC(s) 660 to the End-User Device(s) 109 (step 606). The License SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device(s) 109. If any verification is not successful, the Clearinghouse(s) 105 denies the license to the End-User Device(s) 109 and informs the End-User Device(s) 109. The Clearinghouse(s) 105 also immediately informs the Electronic Digital Content Store(s) 103 of this verification failure. In an alternate embodiment, the Clearinghouse(s) 105 signs the License SC(s) 660 with its

Digital Signature 663.

Detailed Description Text (112):
V. SECURE CONTAINER STRUCTURE

Detailed Description Text (114):
A Secure Container (SC) is a structure that consists of several parts which together define a unit of Content 113 or a portion of a transaction, and which also define related information such as Usage Conditions, metadata, and encryption methods. SC(s) are designed in such a way that the integrity, completeness, and authenticity of the information can be verified. Some of the information in SC(s) may be encrypted so that it can only be accessed after proper authorization has been obtained.

Detailed Description Text (115):
SC(s) include at least one bill of materials (BOM) part which has records of information about the SC(s) and about each of the parts included in the SC(s). A message digest is calculated, using a hashing algorithm such as MD-5, for each part and then included in the BOM record for the part. The digests of the parts are concatenated together and another digest is computed from them and then encrypted using the private key of the entity creating the SC(s) to create a digital signature. Parties receiving the SC(s) can use the digital signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts.

Detailed Description Text (118):
SC(s) may also include a Key Description part. Key Description parts include records that contain the following information about encrypted parts in the SC(s): The name of the encrypted part. The name to use for the part when it is decrypted. The encryption algorithm used to encrypt the part. Either a Key Identifier to indicate the public encryption key that was used to encrypt the part or an encrypted symmetric key that, when decrypted, is used to decrypt the encrypted part. The encryption algorithm used to encrypt the symmetric key. This field is only present when the record in the Key Description part includes an encrypted symmetric key that was used to encrypt the encrypted part. A Key Identifier of the public encryption key that was used to encrypt the symmetric key. This field is only present when the record in the Key Description part includes an encrypted symmetric key and the encryption algorithm identifier of the symmetric key that was used to encrypt the encrypted part.

Detailed Description Text (124):
C. Overview of Secure Container Flow and Processing

Detailed Description Text (125):
Metadata SC(s) 620 are built by Content. Provider(s) 101 and are used to define Content 113 items such as songs. The Content 113 itself is not included in these SC (s) because the size of the Content 113 is typically too large for Electronic Digital Content Store(s) 103 and End-User(s) to efficiently download the containers just for the purpose of accessing the descriptive metadata. Instead, the SC(s) includes an external URL (Uniform Resource Locators) to point to the Content 113. The SC(s) also includes metadata that provides descriptive information about the Content 113 and any other associated data, such as for music, the CD cover art and/or digital audio clips in the case of song Content 113.

Detailed Description Text (131):
If there are any changes required to be made to. the watermarking instructions by the Clearinghouse(s) 105, then the Clearinghouse(s) 105 decrypts the Symmetric Key 623 and then modifies the watermarking instructions and encrypts them again using a new Symmetric Key 623. The Symmetric Key 623 is then re-encrypted using the Public Key 661 of the End-User Device(s) 109. The Clearinghouse(s) 105 also decrypts the

other Symmetric Keys 623 in the SC(s) and encrypts them again with the Public Key 661 of the End-User Device(s) 109. The Clearinghouse(s) 105 builds a License SC(s) 660 that includes the newly encrypted Symmetric Keys 623 and updated watermarking instructions and sends it to the End-User Device(s) 109 in response to the Order SC (s) 650. If the processing of the Order SC(s) 650 does not complete successfully, then the Clearinghouse(s) 105 returns to the End-User Device(s) 109 an HTML page reporting the failure of the authorization process.

Detailed Description Text (133):
D. Metadata Secure Container 620 Format

Detailed Description Text (134):
The following table shows the parts that are included in a Metadata SC(s) 620. Each box in the Parts column is a separate object included in the SC(s) along with the BOM (with the exception of part names that are surrounded by [] characters). The BOM contains a record for each part included in the SC(s). The Part Exists column indicates whether the part itself is actually included in the SC(s) and the Digest column indicates whether a message digest is computed for the part. Some parts may not be propagated when a SC(s) is included in other SC(s) (as determined by the associated template), although the entire original BOM is propagated. This is done because the entire BOM is required by the Clearinghouse(s) 105 to verify the digital signature in the original SC(s).

Detailed Description Text (136):
The following describes the terms that are used in the above Metadata SC(s) table: [Content URL]--A parameter in a record in the Key Description part. This is a URL that points to the encrypted Content 113 in the Content SC(s) 630 that is associated with this Metadata SC(s) 620. The Metadata SC(s) 620 itself does not contain the encrypted Content 113. [Metadata URL]--A parameter in a record in the Key Description part. This is a URL that points to the encrypted metadata in the Content SC(s) 630 that is associated with this Metadata SC(s) 620. The Metadata SC (s) 620 itself does not contain the encrypted metadata. Content ID--A part that defines a unique ID assigned to a Content 113 item. There is more than one Content ID included in this part if the Metadata SC(s) 620 references more than one Content 113 item. Metadata--Parts that contain information related to a Content 113 item such as the artist name and CD cover art in the case of a song. There may be multiple metadata parts, some of which may be encrypted. The internal structure of the metadata parts is dependent on the type of metadata contained therein. Usage Conditions--A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User(s) for use of the Content 113. SC(s) Templates--Parts that define templates that describe the required and optional information for building the Offer, Order, and License SC(s) 660. Watermarking Instructions--A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the Clearinghouse(s) 105 and returned back to the End-User Device(s) 109 within the License SC(s) 660. There is a record in the Key Description part that defines the encryption algorithm that was used to encrypt the watermarking instructions, the output part name to use when the watermarking instructions are decrypted, a base64 encoding of the encrypted Symmetric Key 623 bitstring that is was used to encrypt the watermarking instructions, the encryption algorithm that was used to encrypt the Symmetric Key 623, and the identification of the public key that is required to decrypt the Symmetric Key 623. Clearinghouse(s) Certificate(s)--A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 621 of the Clearinghouse(s) 105. There may be more than one certificate, in which case a hierarchical level structure is used with the highest level certificate containing the public key to open the next lowest level certificate is reached which contains the Public Key 621 of the Clearinghouse(s) 105. Certificate(s)--A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 621 of the entity that created the SC(s). There may be more than one certificate, in which case a

hierarchical level structure is used with the highest level certificate containing the public key to open the next level certificate, and so on, until the lowest level certificate is reached which contains the public key of the SC(s) creator. SC Version--A version number assigned to the SC(s) by the SC Packer Tool. SC ID--A unique ID assigned to the SC(s) by the entity that created the SC(s). SC Type--Indicates the type of SC(s) (e.g. Metadata, Offer, Order, etc.) SC Publisher--Indicates the entity that created the SC(s). Creation Date--Date that the SC(s) was created. Expiration Date--Date the SC(s) expires and is no longer valid. Clearinghouse(s) URL--Address of the Clearinghouse(s) 105 that the End-User Player Application 195 should interact with to obtain the proper authorization to access the Content 113. Digest Algorithm ID--An identifier of the algorithm used to compute the digests of the parts. Digital Signature Alg ID--An identifier of the algorithm used to encrypt the digest of the concatenated part digests. This encrypted value is the digital signature. Digital Signature--A digest of the concatenated part digests encrypted with the public key of the entity that created the SC(s). Output Part--The name to assign to the output part when an encrypted part is decrypted. RSA and RC4--Default encryption algorithms used to encrypt the Symmetric Keys 623 and data parts. Enc Sym Key--A base64 encoding of an encrypted key bitstring that, when decrypted, is used to decrypt a SC(s) part. CH Pub Key--An identifier that indicates that the Clearinghouse's 105 Public Key 621 was used to encrypt the data.

Detailed Description Text (137):
E. Offer Secure Container 641 Format

Detailed Description Text (140):
Metadata SC(s) BOM--The BOM from the original Metadata SC(s) 620. The record in the Offer SC(s) 641 BOM includes the digest of the Metadata SC(s) 620 BOM. Additional and Overridden Fields--Usage conditions information that was overridden by the Electronic Digital Content Store(s) 103. This information is validated by the Clearinghouse(s) 105, by means of the received SC(s) templates, to make sure that anything that the Electronic Digital Content Store(s) 103 overrides is within the scope of its authorization. Electronic Digital Content Store(s) Certificate--A certificate provided to the Electronic Digital Content Store(s) 103 by the Clearinghouse(s) 105 and signed by the Clearinghouse(s) 105 using its private key. This certificate is used by the End-User Player Application 195 to verify that the Electronic Digital Content Store(s) 103 is a valid distributor of Content 113. The End-User Player Application 195 and Clearinghouse(s) 105 can verify that the Electronic Digital Content Store(s) 103 is an authorized distributor by decrypting the certificate's signature with the Clearinghouse's 105 Public Key 621. The End-User Player Application 195 keeps a local copy of the Clearinghouse's 105 Public Key 621 that it receives as part of its initialization during installation.

Detailed Description Text (141):
F. Transaction Secure Container 640 Format

Detailed Description Text (143):
The following describes the terms that are used in the above Transaction SC(s) 640 that were not previously described for another SC(s): Transaction ID 535--An ID assigned by the Electronic Digital Content Store(s) 103 to uniquely identify the transaction. End-User(s) ID--An identification of the End-User(s) obtained by the Electronic Digital Content Store(s) 103 at the time the End-User(s) makes the buying selection and provides the credit card information. End-User(s)' Public Key--The End-User(s)' Public Key 661 that is used by the Clearinghouse(s) 105 to re-encrypt the Symmetric Keys 623. The End-User(s)' Public Key 661 is transmitted to the Electronic Digital Content Store(s) 103 during the purchase transaction. Offer SC(s)--Offer SC(s) 641 for the Content 113 items that were purchased. The Offer SC (s) do not have digests computed because each container can be validated individually. Offer SC(s) BOMs--BOM parts of the Offer SC(s) 641 that are included as parts in the Transaction SC(s) 640. The Transaction SC(s) 640 BOM has a record

for each of the Offer SC(s) 641 BOM parts. The record includes a digest of the BOM part and a parameter that identifies the name of the Offer SC(s) 641 part that is associated with this Offer SC(s) 641 BOM part. After each Offer SC(s) 641 is unpacked by the packer, a digest is computed for its BOM and compared with the digest of its associated Offer SC(s) 641 BOM record in the Transaction SC(s) 640. If the digests match, then the BOMs are identical and the appropriate Offer SC(s) 641 was really included in the Transaction SC(s) 640. If the digest do not match, then the SC(s) is not valid. Selections of Content Use--An array of Usage Conditions for each Content 113 item being purchased by the End-User(s). There is an entry for each Offer SC(s) 641. HTML to Display--One or more HTML pages that the End-User Player Application 195 displays in the Internet browser window upon receipt of the Transaction SC(s) 640 or during the interaction between the End-User Device(s) 109 and the Clearinghouse(s) 105. When the End-User Device(s) 109 receives a Transaction SC(s) 640, the following steps may be performed to verify the integrity and authenticity of the SC(s): 1. Verify the integrity of the Electronic Digital Content Store(s) 103 certificate using the Public Key 621 of the Clearinghouse(s) 105. The Public Key 621 of the Clearinghouse(s) 105 was stored at the End-User Device(s) 109 after it was received as part of the initialization of the End-User Player Application 195 during its installation process. 2. Verify the Digital Signature 643 of the SC(s) using the public key from the Electronic Digital Content Store(s) 103 certificate. 3. Verify the hashes of the SC(s) parts. 4. Verify the integrity and authenticity of each Offer SC(s) 641 included in the Transaction SC(s) 640. 5. Compute the hashes of BOMs from each Offer SC(s) 641 and compare them against the hashes of the Offer SC(s) 641 BOMs that are included as parts in the Transaction SC(s) 640.

Detailed Description Text (144):
G. Order Secure Container 650 Format

Detailed Description Text (147):
H. License Secure Container 660 Format

Detailed Description Text (148):
The following table shows the parts that are included in the License SC(s) 660 as well as its BOM. As shown in the Key Description part, the Symmetric Keys 623 that are required for decrypting the watermarking instructions, Content 113, and Content 113 metadata have been re-encrypted by the Clearinghouse(s) 105 using the End-User (s)' Public Key 661. When the End-User Device(s) 109 receives the License SC(s) 660 it decrypts the Symmetric Keys 623 and use them to access the encrypted parts from the License SC(s) 660 and the Content SC(s) 630.

Detailed Description Text (149):
The following describes the terms that are used in the above License SC(s) 660 that were not previously described for another SC(s): EU Pub Key--An identifier that indicates that the End-User(s)' Public Key 661 was used to encrypt the data. Order SC(s) 650 ID--The SC(s) ID taken from the Order SC(s) 650 BOM. Certificate Revocation List--An optional list of certificate IDs which were previously issued and signed by the Clearinghouse(s) 105, but are no longer considered to be valid. Any SC(s) that have a signature which can be verified by a certificate that is included in the revocation list are invalid SC(s). The End-User Player Application 195 stores a copy of the Clearinghouse's 105 certificate revocation list on the End-User Device(s) 109. Whenever a revocation list is received, the End-User Player Application 195 replaces its local copy if the new one is more up to date. Revocation lists includes a version number or a time stamp (or both) in order to determine which list is the most recent.

Detailed Description Text (150):
I. CONTENT SECURE CONTAINER FORMAT

Detailed Description Text (154):

VI. SECURE CONTAINER PACKING AND UNPACKING

Detailed Description Text (165):
The following record type is used within a Key Description part and is defined as follows: K encrypted_part_name; result_part_name; part_encryption_algorithm_identifier; public_key_identifier_or_encrypted_key comprising [key_encryption_algorithm_identifier and key_public_key_identifier]. A K record specifies an encrypted part that may be included in this SC(s) or may be included in another SC(s) that is referred to by this record. The encrypted_part_name is either the name of a part in this SC(s) or a URL pointing to the name of the encrypted part in another SC(s). The result_part_name is the name that is given to the decrypted part. The part_encryption_algorithm_identifier indicates the encryption algorithm that was used to encrypt the part. The public_key_identifier_or_encrypted_key is either an identifier of the key that was used to encrypt the part or a base64 encoding of the encrypted Symmetric Key 623 bitstring that was used to encrypt the part. The key_encryption_algorithm_identifier and the key_public_key_identifier are only specified when the public_key_identifier_or_encrypted_key is an encrypted Symmetric Key 623. In this case the key_encryption_algorithm_identifier indicates the encryption algorithm that was used to encrypt the Symmetric Key 623 and the key_public_key_identifier indicates the encryption key that was used to encrypt the Symmetric Key 623.

Detailed Description Text (170):
An Electronic Digital Content Store(s) 103 that wants to participate as a seller of Content 113 in the Secure Digital Content Electronic Distribution System 100 makes a request to one or more of the Digital Content Provider(s) 101 that provide Content 113 to the Secure Digital Content Electronic Distribution System 100. There is no definitive process for making the request so long as the two parties come to an agreement. After the digital content label such as a Music Label e.g. Sony, Time-Warner, etc. decides to allow the Electronic Digital Content Store(s) 103 to sell its Content 113, the Clearinghouse(s) 105 is contacted, usually via E-mail, with a request that the Electronic Digital Content Store(s) 103 be added to the Secure Digital Content Electronic Distribution System 100. The digital content label provides the name of the Electronic Digital Content Store(s) 103 and any other information that may be required for the Clearinghouse(s) 105 to create a digital certificate for the Electronic Digital Content Store(s) 103. The digital certificate is sent to the digital content label in a secure fashion, and then forwarded by the digital content label to the Electronic Digital Content Store(s) 103. The Clearinghouse(s) 105 maintains a database of digital certificates that it has assigned. Each certificate includes a version number, a unique serial number, the signing algorithm, the name of the issuer (e.g., the name of Clearinghouse(s) 105), a range of dates for which the certificate is considered to be valid, the name Electronic Digital Content Store(s) 103, the public key of the Electronic Digital Content Store(s) 103, and a hash code of all of the other information signed using the private key of the Clearinghouse(s) 105. Entities that have the Public Key 621 of the Clearinghouse(s) 105 can validate the certificate and then be assured that a SC(s) with a signature that can be validated using the public key from the certificate is a valid SC(s).

Detailed Description Text (171):
After the Electronic Digital Content Store(s) 103 has received its digital certificate that was created by the Clearinghouse(s) 105 and the necessary tools for processing the SC(s) from the digital content label, it can begin offering Content 113 that can be purchased by End-User(s). The Electronic Digital Content Store(s) 103 includes its certificate in the Offer SC(s) 641 and the Transaction SC (s) 640 and signs the SC(s) using its Digital Signature 643. The End-User Device(s) 109 verifies that the Electronic Digital Content Store(s) 103 is a valid distributor of Content 113 on the Secure Digital Content Electronic Distribution System 100 by first checking the digital certificate revocation list and then using

the Public Key 621 of the Clearinghouse(s) 105 to verify the information in the digital certificate for the Electronic Digital Content Store(s) 103. A digital certificate revocation list is maintained by the Clearinghouse(s) 105. The revocation list is included as one of the parts in every License SC(s) 660 that is created by the Clearinghouse(s) 105. End-User Device(s) 109 keep a copy of the revocation list on the End-User Device(s) 109 so they can use it as part of the Electronic Digital Content Store(s) 103 digital certificate validation. Whenever the End-User Device(s) 109 receives a License SC(s) 660 it determines whether a new revocation list is included and if so, the local revocation list on the End-User Device(s) 109 is updated.

Detailed Description Text (176):
The Clearinghouse(s) 105 begins the validation of Order SC(s) 650 by verifying the digital signatures, then the Clearinghouse(s) 105 verifies the integrity of the Order SC(s) 650 parts. To validate the digital signature, first the Clearinghouse (s) 105 decrypts the Contents 631 of the signature itself using the Public Key 661 of End-User Device(s) 109 included in the Order SC(s) 650. Then, the Clearinghouse (s) 105 calculates the digest of the concatenated part digests of the Order SC(s) 650 and compares it with the digital signature's decrypted Content 113. If the two values match, the digital signature is valid. To verify the integrity of each part, the Clearinghouse(s) 105 computes the digest of the part and compares it to the digest value in the BOM. The Clearinghouse(s) 105 follows the same process to verify the digital signatures and part integrity for the Metadata and Offer SC(s) 641 parts included within the Order SC(s) 650.

Detailed Description Text (177):
The process of verification of the Transaction and Offer SC(s) 641 digital signatures also indirectly verifies that the Electronic Digital Content Store(s) 103 is authorized by the Secure Digital Content Electronic Distribution System 100. This is based on the fact that the Clearinghouse(s) 105 is the issuer of the certificates. The Clearinghouse(s) 105 would be able to successfully verify the digital signatures of the Transaction SC(s) 640 and Offer SC(s) 641 using the public key from the Electronic Digital Content Store(s) 103, only if the entity signing the SC(s) has ownership of the associated private key. Only the Electronic Digital Content Store(s) 103 has ownership of the private key. Notice that the Clearinghouse(s) 105 does not need to have a local database of the Electronic Digital Content Store(s) 103.

Detailed Description Text (180):
Processing of the encrypted Symmetric Keys 623 and of the watermarking instructions is done by the Clearinghouse(s) 105 after authenticity and the integrity check of the Order SC(s) 650, the validation of the Electronic Digital Content Store(s) 103, and the validation of the Store Usage Conditions 519 have been completed successfully. The Metadata SC(s) 620 portion of the Order SC(s) 650 typically has two Symmetric Keys 623 located in the Key Description part that were encrypted using the Public Key 621 of the Clearinghouse(s) 105. Encryption of the Symmetric Keys 623 is done by the Content Provider(s) 101 when the Metadata SC(s) 620 was created.

Detailed Description Text (181):
One Symmetric Key 623 is used for decrypting the watermarking instructions and the other for decrypting the Content 113 and any encrypted metadata. The watermarking instructions are included within the Metadata SC(s) 620 portion in the Order SC(s) 650. The Content 113 and encrypted metadata are in the Content SC(s) 630 at a Content Hosting Site(s) 111. The URL and part names of the encrypted Content 113 and metadata parts, within the Content SC(s) 630, are included in the Key Description part of the Metadata SC(s) 620 portion of the Order SC(s) 650. The Clearinghouse(s) 105 uses its private key to decrypt the Symmetric Keys 623 and then encrypts each of them using the Public Key 661 of the End-User Device(s) 109. The Public Key 661 of the End-User Device(s) 109 is retrieved from the Order SC(s)

650. The new encrypted Symmetric Keys 623 is included in the Key Description part of the License SC(s) 660 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109.

Detailed Description Text (290):
A usage condition defines: 1. the compression encoded version of the Content 113 to which this usage condition applies. 2. the type of user covered by this usage condition (e.g., business, private consumer) 3. whether this usage condition allows for the purchase or the rental of the Content 113. For a rental transaction: the measurement unit which is used to limit the term of the rental (e.g., days, plays). the number of the above units after which the Content 113 will no longer play. For a purchase transaction: the number of playable copies the End-User(s) is allowed to make. onto what kinds of media can he/she make those copies (e.g., CD-Recordable (CD-R), MiniDisc, Personal Computer). 4. the period of time during which the purchase/rental transaction is allowed to occur (i.e., an End-User(s) can purchase/rent under the terms of this usage condition only after the beginning availability date and before the last date of availability). 5. the countries from which an End-User(s) can transact this purchase (or rental). 6. the price of the purchase/rental transaction under this usage condition 7. the watermarking parameters. 8. the types of events which require notification of the Clearinghouse (s) 105.

Detailed Description Text (330):
Metadata SC(s) 620 received into a new content directory via FTP from the Content Dispersement Tool is processed by the Content Promotions Web Site 156. These containers can be opened with the SC(s) Preview Tool to display or extract information from the container. This information can then be used to update HTML Web pages and/or add information to a searchable database maintained by this service. The SC(s) Preview Tool is actually a subset of the Content Acquisition Tool used by the Electronic Digital Content Store(s) 103 to open and process Metadata SC(s) 620. See the Content Acquisition Tool section for more details. The Metadata SC(s) 620 file should then be moved to a permanent directory maintained by the Content Promotions Web Site 156.

Detailed Description Text (331):
Once the Metadata SC(s) 620 has been integrated into the Content Promotions Web Site 156, its availability is publicized. The Content Provider(s) 101 can send a notification to all subscribing Electronic Digital Content Store(s) 103 as each new Metadata SC(s) 620 is added to the site or can perform a single notification daily (or any defined periodicity) of all Metadata SC(s) 620 added that day (or period). This notification is performed via a standard HTUP exchange with the Electronic Digital Content Store(s) 103 Web Server by sending a defined CGI string containing parameters referencing the Metadata SC(s) 620 added. This message is handled by the Notification Interface Module of the Electronic Digital Content Store(s) 103 which is described later.

Detailed Description Text (357):
The tools for the Secure Digital Content Electronic Distribution have been designed to allow integration of sale of electronic downloadable Content 113 into typical implementations of web based Electronic Digital Content Store(s) 103 (i.e. Columbia House online, Digital Content Boulevard, @Tower) and equivalent with minimal change to their current Content 113 retailing paradigm. Several methods of integration are possible and in the preferred embodiment, the Electronic Digital Content Store(s) 103 provides support for all product searches, previews, selections (shopping cart), and purchases. Each Electronic Digital Content Store(s) 103 establishes customer loyalty with its customers and continues to offer its own incentives and market its products as it does today. In the Secure Digital Content Electronic Distribution System 100, it would simply need to indicate which products in its inventory are also available for electronic download and allow its customers to select the electronic download option when making a purchase selection. In another

embodiment the customer's shopping cart could contain a mixture of electronic (Content 113) and, physical media selections. After the customer checks out, and the Electronic Digital Content Store(s) 103 has completed, the financial settlement and logged or notified its shipping and handling functions to process the physical merchandise purchased, the commerce handling function of the Electronic Digital Content Store(s) 103 then calls the Transaction Processor Module 175 to handle all electronic downloads. It simply passes the required information and all processing from that point on is handled by the toolset for the Secure Digital Content Electronic Distribution System 100. In another embodiment, other methods of transaction handling are also possible using tools for the Secure Digital Content Electronic Distribution System 100 to handle the financial settlement should the Electronic Digital Content Store(s) 103 wish to sell downloadable merchandise only or to segregate the financial settlement of physical and downloadable merchandise.

Detailed Description Text (358):
To handle the downloading of merchandise, the Electronic Digital Content Store(s) 103 is given a Product ID (not shown) for each downloadable product that it acquires from the Content Promotions Web Site 156 for the Content Provider(s) 101. This Product ID is associated to a customer's purchase selection to the downloadable product. The Product ID is what the Electronic Digital Content Store (s) 103 passes to the Transaction Processor Module 175 to identify the product that the user has purchased. The SC(s) (Offer SC(s) 641) that were created to describe the products, are isolated from the Electronic Digital Content Store(s) 103 and kept in an Offer Database 181 in an effort to simplify management of these objects and make their existence transparent to the Electronic Digital Content Store(s) 103.

Detailed Description Text (359):
The Transaction Processor Module 175 and other additional functions are provided as web server side executables (i.e. CGI and NSAPI, ISAPI callable functions). These functions handle run time processing for End-User(s) interactions and optional interactions with the Clearinghouse(s) 105. These functions interact with the web server's commerce services to create and download to the End-User Device(s) 109 the files necessary to initiate the Content 113 download process. They also handle optional interactions to provide authorizations and accept notifications of completion of activities.

Detailed Description Text (367):
One important piece of information provided in the extracted'data is the Product ID. This Product ID is what the commerce handling function for the Electronic Digital-Content Store(s) 103 needs to identify to the Transaction Processor Module 175 (for more information refer to Transaction Processing section), the Content 113 that the user has purchased. The Transaction Processor Module 175 uses this Product ID to properly retrieve the appropriate Offer SC(s) 641 from the Offer Database 181 for subsequent download to the End-User Device(s) 109. The Electronic Digital Content Store(s) 103 has full control over how it presents the offer of downloadable Content 113 on its site. It only needs to retain a cross reference of the Content 113 being offered to this Product ID to properly interface with the tools for the Secure Digital Content Electronic Distribution System 100. Providing this information here, allows the Electronic Digital Content Store(s) 103 to integrate this product or Content 113 into its inventory and sales pages (database) in parallel with the Offer SC(s) 641 creation process since both processes uses the same Product ID to reference the product This is described further below.

Detailed Description Text (372):
Once the Offer SC(s) 641 is created, it is stored in an Offer Database 181 and is indexed with the Product ID pre-assigned in the Metadata SC(s) 620. This Product ID is used later by the Electronic Digital Content Store(s) 103 to identify the downloadable Content 113 being purchased by a customer when interfacing with the Offer Database 181 to retrieve the Offer SC(s) 641 for packaging and transmittal to

the End-User(s). See the Transaction Processor Module 175 section for more details.

Detailed Description Text (373):
In another embodiment, the Electronic Digital Content Store(s) 103 hosts the Content SC(s) 641 at his site. This embodiment requires changes to the Offer SC(s) 641 such as the replacement of the URL of the Content Hosting Site(s) 111 with the URL of the Electronic Digital Content Store(s) 103. 3. Transaction Processing Module 175

Detailed Description Text (374):
Electronic Digital Content Store(s) 103 directs billing to Clearinghouse(s) 105. There are two basic modes for processing End-User(s) purchase requests for downloadable Content 113. If the Electronic Digital Content Store(s) 103 does not wish to handle the financial settlement of the purchase and has no special promotions or incentives governing the sale of the merchandise and does not use a shopping cart metaphor for batching the purchase requests, it may opt to provide links on its Content 113 download pages directly to the Offer SC(s) 641 files. These Offer SC(s) 641 would have to have been built with retail pricing information included in the metadata. Also included in the Offer SC(s) 641 is a special HTML offer page presenting the purchase options with terms and conditions of the sale. This page is built from a template created when the Offer SC(s) 641 was built. When the End-User(s) clicks on the direct link to the Offer SC(s) 641, the Offer SC(s) 641 is downloaded to the browser End-User Device(s) 109 launching a helper application which opens the container and present the offer page included in the Offer SC(s) 641. This page contains a form to collect customer information including credit card information and purchase option selection. The form then gets submitted directly to the Clearinghouse(s) 105 for financial settlement and processing. Optionally, this form may contain the fields needed to use the End-User (s)' credit information or industry standard local transaction handler.

Detailed Description Text (375):
An embodiment where the Electronic Digital Content Store(s) 103 handles billing is now described. The more typical mode of handling purchase requests is to allow the Electronic Digital Content Store(s) 103 to process the financial settlement and then submit the download authorization to the End-User(s). This method allows the Electronic Digital Content Store(s) 103 to integrate sale of downloadable Content 113 with other merchandise offered for sale at his site, allows batch processing of purchase requests with only one consolidated charge to the customer (via a shopping cart metaphor) instead of individual charges for each download request, and allows the Electronic Digital Content Store(s) 103 to directly track his customers buying patterns and offer special promotions and club options. In this environment, the offer of downloadable Content 113 is included in his shopping pages which get added to a shopping cart when selected by the End-User(s) and get processed and financially settled as is done in the Electronic Digital Content Store(s)' 103 current shopping model. Once the financial settlement is completed, the commerce handling process of the Electronic Digital Content Store(s) 100 then calls the Transaction Processor Module 175 to complete the transaction.

Detailed Description Text (376):
Transaction Processor Module 175

Detailed Description Text (377):
The role of the Transaction Processor Module 175 is to put together the information needed by the End-User Device(s) 109 to initiate and process the download of the Content 113 purchased. This information is packaged into a Transaction SC(s) 640 which is sent back to the End-User Device(s) 109 by the Web Server as the response to the purchase submission. The Transaction Processor Module 175 requires three pieces of information from the commerce handling process of the Electronic Digital Content Store(s) 103: the Product IDs for the Content 113 purchased, Transaction

Data 642, and an HTML page acknowledging the purchase settlement.

Detailed Description Text (383):
The final parameter required by the Transaction Processor Module 175 is the HTML page acknowledging the purchase settlement. The purpose of this is to allow the Electronic Digital Content Store(s) 103 to respond to the End-User(s) with an acknowledgment of the financial settlement and whatever other information he wishes to include in the response. This HTML page is included in the Transaction SC(s) 640 and is displayed in the browser window of the End-User Device(s) 109 when the Transaction SC(s) 640 is received and processed.

Detailed Description Text (385):
When the Transaction Processor Module 175 is called with the required parameters, it builds a Transaction SC(s) 640 containing the Transaction Data 642, the transaction acknowledgment HTML page, other required security features of the SC (s), and retrieves and imbeds the Offer SC(s) 641 associated with the purchase. It also logs information about this transaction for later use by the Notification Interface. Module 176 and the Account Reconciliation Tool 179.

Detailed Description Text (386):
4. Notification Interface Module 176

Detailed Description Text (387):
The Notification Interface Module 176 is a Web Server side executable routine (CGI or function callable by NSAPI, ISAPI or equivalent). It handles optional requests and notifications from the Clearinghouse(s) 105, the End-User Device(s) 109, the Content Hosting Site(s) 111, and the Content Provider(s) 101. The events that the Electronic Digital Content Store(s) 103 can optionally request notification for are: Notification from the Clearinghouse(s) 105 that the End-User Device(s) 109 requesting an encryption Key 623 and the Clearinghouse(s) 105 is releasing the encryption Key. 623 for three specified Content 113. This notification can optionally be configured to require authentication from the Electronic Digital Content Store(s) 103 prior to the encryption Key 623 being sent to the End-User Device(s) 109. Notification from the Content Hosting Site(s) 111 that the Content SC(s) 630 has been sent to the End-User Device(s) 109. Notification from the End-User Device(s) 109 that the Content SC(s) 630 and the License SC(s) 660 have been received and successfully used to process the Content 113 or was found to be corrupt. Notification from the Content Provider(s) 101 that new Content 113 has been placed in the Content Promotions Web Site 156.

Detailed Description Text (390):
All of these notifications result in entries being made to the Transaction Log 178. If the Electronic Digital Content Store(s) 103 wishes to perform his own processing on these notifications, he can intercept the CGI call, perform his unique function and then optionally pass the request on to the Notification Interface Module 176.
5. Account Reconciliation Tool 179

Detailed Description Text (405):
The Player Application 195 and the Helper Application 198 are packaged into a self installing executable program which is available for download from many web sites. The Clearinghouse(s) 105 acts as a central location which hosts the master download page at a public web site. It contains links to the locations from which the installation package can be downloaded. The installation package is available at all Content Hosting Site(s) 111 to provide geographic dispersal of the download requests. Each participating Electronic Digital Content Store(s) 103 can also make the package available for download from their site or may just provide a link to the master download page at the public web site of the Clearinghouse(s) 105.

Detailed Description Text (407):
As part of the installation, a Public/Private Key 661 pair is created for the End-

User Device(s) 109 for use in processing Order and License SC(s) 660. A random Symmetric Key (Secret User Key) is also generated for use in protecting song encryption keys in the License Database 197. The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple locations throughout the End-User(s)' computer. This area of the code is protected with Tamper Resistant Software technology so as not to divulge how the key is segmented and where it is stored. Preventing access to this key by even the End-User(s) helps to prevent piracy or sharing of the Content 113 with other computers. See the SC(s) Processor 192 section for more details on how these keys are used.

Detailed Description Text (411):
C. Secure Container Processor 192

Detailed Description Text (414):
When the scheduled download time occurs or if immediate download was requested, the SC(s) Processor 192 creates Order SC(s) 650 from information in the Transaction SC (s) 640, Offer SC(s) 641, and the Public Key 661 of the End-User(s) generated at install time. This Order SC(s) 650 is sent via HTTP request through the Browser to the Clearinghouse(s) 105. When the Clearinghouse(s) 105 returns the License SC(s) 660, the Helper Application 198 is re-invoked to process the License SC(s) 660. The License SC(s) 660 is then opened and the URL of the Content Hosting Site(s) 111 is extracted from the referenced Order SC(s) 650. The License SC(s) 660 is then sent to the specified Content Hosting Site 111, via http request through the Browser, requesting download of the Content SC(s) 630. When the Content SC(s) 630 comes back to the Browser, the Helper Application 198 is re-invoked again. The SC(s) Processor 192 displays the name of the Content 113 being downloaded along with a download progress indicator and an estimated time to completion.

Detailed Description Text (415):
As the Content 113 is being received by the SC(s) Processor 192, it loads the Content 113 data into memory buffers for decryption. The size of the buffers depends on the requirements of the encryption algorithm and watermarking technology 193 and is the minimum size possible to reduce the amount of unencrypted Content 113 exposed to hacker code. As a buffer is filled, it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the License SC(s) 660, which itself is first decrypted using the Private Key. The decrypted buffer is then passed to the watermarking function.

Detailed Description Text (416):
The watermarking 193 extracts the watermarking instructions from the License SC(s) 660 and decrypt the instructions using the Private Key of the End-User(s). The watermarking data is then be extracted from the License SC(s) 660 which includes transaction information such as the purchaser's name as registered with the Electronic Digital Content Store(s) 103 from which this Content 113 was purchased or derived from the credit card registration information if the Electronic Digital Content Store(s) 103 does not provide a registration function. Also included in the watermark is the purchase date and the Transaction ID 535 assigned by the Electronic Digital Content Store(s) 103 to reference the specific records logged for this transaction. The Store Usage Conditions 519 are also included to be used by the Copy Control of the Player Application 195. The watermarking instructions determines which specific content buffers the watermark is written to.

Detailed Description Text (431):
This set is grouped into subgroups, starting with the components used to present End-User Display 1510 and handle controls called End-User Controls 1511 used for such low-level functions as audio playback , and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special function groupings (Play-list, Digital Content Library), and then object-container components used for grouping and placing of those lower-level components.

Detailed Description Text (437):
Play-list of display container Play-list Management button Play-list Management window Digital Content search button Digital Content search Definition object Digital Content search Submit button Digital Content search Results object Copy Selected Search Result Item To Play-list button Play-list object (editable) Play-list Save button Play-list Play button Play-list Pause button Play-list Restart button Create CD from Play-list button and more.

Detailed Description Text (438):
Display of Digital Content Library 196 Digital content library button Digital content librarian window Digital content categories button Digital content categories object By-artist button By-genre button By-label button By-category button Delete button Add-to-Play-list button Copy to CD button Song List object Song List display container and more Containers and Misc. Player window container Audio controls container Metadata controls container Metadata display container Toolbar container object Sample button Download button Purchase button Record button Player Name object Label/Provider/Store Advertisement object Label/Provider/Store URL button Artist URL Button and more 3. Copy/Play Management Components 1504

Detailed Description Text (446):
Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly derived from the metadata associated with the Content 113 being played or searched. These Variable Objects are made available to the End-User Device(s) 109 by way of the End-User Display 1510 and received input from the End-User Controls 1511. All objects are configurable, and the layouts of all containers are customizable. These objects may be implemented in C/C++, Java or any equivalent object oriented language.

Detailed Description Paragraph Table (3):
Step Process 301 Sender generates a random symmetric key and uses it to encrypt the content. 302 Sender runs the encrypted content through a hash algorithm to produce the content digest. 303 Sender encrypts the symmetric key using the recipient's public key. PB RECPNT refers to the recipient's public key. 304 Sender runs the encrypted symmetric key through the same hash algorithm used in step 2 to produce the symmetric key digest. 305 Sender runs the concatenation of the content digest and symmetric key digest through the same hash algorithm used in step 2 to produce the SC(s) digest. 306 Sender encrypts the SC(s) digest with the sender's private key to produce the digital signature for the SC(s). PV SENDER refers to the sender's private key. 307B Sender creates a SC(s) file that includes the encrypted content, encrypted symmetric key, content digest, symmetric key digest, sender's certificate, and SC(s) signature. 307A Sender must have obtained the certificate from a certification authority prior to initiating secure communications. The certification authority includes in the certificate the sender's public key, the sender's name and signs it. PV CAUTHR refers to the certifications authority's private key. Sender transmits the SC(s) to the recipient.

Detailed Description Paragraph Table (4):
Step Process 408 Recipient receives the SC(s) and separates its parts. 409 Recipient verifies the digital signature in the sender's certificate by decrypting it with the public key of the certification authority. If the certificate's digital signature is valid, recipient acquires the sender's public key from the certificate. 410 Recipient decrypts the SC(s) digital signature using the sender's public key. This recovers the SC(s) digest. PB SENDER refers to the sender's public key. 411 Recipient runs the concatenation of the received content digest and encrypted key digest through the same hash algorithm used by the sender to compute the SC(s) digest. 412 Recipient compares the computed SC(s) digest with the one recovered from the sender's digital signature. If they are the same, recipient confirms that the received digests have not been altered and continues with the

decryption process. If they are not the same, recipient discards the SC(s) and notifies the sender. 413 Recipient runs the encrypted symmetric key through the same hash algorithm used in step 411 to compute the symmetric key digest. 414 Recipient compares the computed symmetric key digest with the one received in the SC(s). If it is the same, recipient knows that the encrypted symmetric key has not been altered. Recipient continues with the decryption process. If not valid, recipient discards the SC(s) and notifies the sender. 415 Recipient runs the encrypted content through the same hash algorithm used in step 411 to compute the content digest. 416 Recipient compares the computed content digest with the one received in the SC(s). If it is the same, recipient knows that the encrypted content has not been altered. Recipient then continues with the decryption process. If not valid, recipient discards the SC(s) and notifies the sender. 417 Recipient decrypts the encrypted symmetric key using the recipient's private key. This recovers the symmetric key. PV RECPNT refers to the recipient's private key. 418 Recipient uses the symmetric key to decrypt the encrypted content. This recovers the content.

Detailed Description Paragraph Table (5):
Step Process 121 A uncompressed PCM audio file is provided as Content 113 by the Content Provider(s) 101. Its filename is input into the Work Flow Manager 154 Tool along with the Content Provider(s)' 101 unique identifier for the Content 113. 122 Metadata is captured from the Content Provider(s)' Database 160 by the Content Information Processing Subsystem using the Content Provider(s)' 101 unique identifier for the Content 113 and information provided by the Database Mapping Template. 123 The Work Flow Manager Tool 154 is used to direct the content flow through the acquisition and preparation process at the Content Provider(s) 101. It can also be used to track the status of any piece of content in the system at any time. 124 The Usage Conditions for the Content 113 are entered into the Content Information Processing Subsystem, this can be done either manually or automatically. This data includes copy restriction rules and any other business rules deemed necessary. All of the metadata entry can occur in parallel with the Audio Processing for the data. 125 The Watermarking Tool is used to hide data in the Content 113 that the Content Provider(s) 101 deems necessary to identify the content. This could include when it was captured, where it came from (this Content Provider(s) 101), or any other information specified by the Content Provider(s) 101. The Content 113 Encoding Tool performs equalization, dynamic range adjustments and re-sampling to the Content 113 as necessary for the different compression levels supported. The Content 113 is compressed using the Content 113 Encoding Tool to the desired compression levels. The Content 113 can then be played back to verify that the compression produces the required level of Content 113 quality. If necessary the equal- ization, dynamic range adjustments, compression and playback quality checks can be performed as many times as desired. The Content 113 and a subset of its metadata is encrypted with a Symmetric Key by the SC Packer. This tool then encrypts the key using the Public Key of the Clearinghouse(s) 105 to produce an Encrypted Symmetric Key. This key can be transmitted any- where without comprising the security of the Content 113 since the only entity that can decrypt it is the Clearinghouse(s) 105. 126 The Encrypted Symmetric Key, metadata and other information about the Content 113 is then packed into a Metadata SC by the SC Packer Tool 152. 127 The encrypted Content 113 and metadata are then packed into a Content SC. At this point the processing on the Content 113 and metadata is complete. 128 The Metadata SC(s) is then sent to the Content Promotions Web Site 156 using the Content Disbursement Tool (not shown). 129 The Content Disbursement Tool sends the Content SC(s) to the Content Hosting Site(s) 111. The Content Hosting Site(s) can reside at the Content Provider(s) 101, the Clearinghouse(s) 105 or a special location dedicated for Content Hosting. The URL for this site is part of the metadata that was added to the Metadata SC. 130 The Content Promotions Web Site 156 notifies Electronic Digital Content Store(s) 103 of new Content 113 that is added to the System 100. 131 Using the Content Acquisition Tool, Electronic Digital Content Store(s) 103 then download the Metadata SCs that correspond to the Content 113 they wish to sell. 132 The Electronic Digital Content Store(s) 103 will

use the Content Acquisition Tool to pull out any data from the Metadata SC(s) that they want to use to promote the Content 113 on their Web Site. Access to portions of this metadata can be secured and charged for if desired. 133 The Usage Conditions for the Content 113, specific to this Electronic Digital Content Store (s) 103, are entered using the Content Acquisition Tool. These Usage Conditions include the retail prices and copy/play restrictions for the different compression levels of the Content 113. 134 The Electronic Digital Content Store(s) 103 specific Usage Conditions and the original Metadata SC(s) are packed into an Offer SC by the SC Packer Tool. 135 After the Electronic Digital Content Store(s) 103 Web Site is up- dated, the Content 113 is available to End-User(s) surfing the Web. 136 When an End-User(s) finds Content 113 that they want to buy, they click on a content icon, such as a music icon, and the item is added to his/her shopping cart which is maintained by the Electronic Digital Content Store(s) 103. When the End-User(s) completes shopping they submit the purchase request to the Electronic Digital Content Store(s) 103 for processing. 137 The Electronic Digital Content Store(s) 103 then interacts with credit card clearing organizations to place a hold on the funds in the same way they do business today. 138 Once the Electronic Digital Content Store(s) 103 receives the credit card authorization number back from the credit card clearing organization, it stores this into a database and invokes the SC Packer Tool to build a Transaction SC. This Transaction SC includes all of the Offer SCs for the Content 113 that the End-User(s) has purchased, a Transaction ID that can be tracked back to the Electronic Digital Content Store(s) 103, information that identifies the End-User(s), compression levels, Usage Conditions and the price list for the songs purchased. 139 This Transaction SC is then transmitted to the End-User Device(s) 109. 140 When the Transaction SC arrives on the End-User Device(s) 109, it kicks off the End-User Player Application 195 which opens the Transaction SC and acknowledges the End-User's purchase. The End-User Player Application 195 then opens the individual Offer SCs and informs the user with an estimate of the download time. It then asks the user to specify when they want to download the Content 113. 141 Based on the time the End-User(s) requested the download, the End-User Player Application 195 will wake up and initiate the start of the download process by building a Order SC that contains among other things the Encrypted Symmetric Key for the Content 113, the Transaction ID, and End-User(s) information. 142 This Order SC is then sent to the Clearinghouse(s) 105 for processing. 143 The Clearinghouse(s) 105 receives the Order SC, opens it and verifies that none of the data has been tampered with. The Clearinghouse(s) 105 validates the Usage Conditions purchased by the End-User(s). These Usage Conditions must comply with those specified by the Content Provider(s) 101. This information is logged in a database. 144 Once all the checks are complete, the Encrypted Symmetric Key is decrypted using the private key of the Clearinghouse(s) 105. The Symmetric Key is then encrypted using the public key of the End-User(s). This new Encrypted Symmetric Key is then packaged into a License SC by the SC Packer. 145 The License SC is then transmitted to the End-User(s). 146 When the License SC is received at the End-User Device(s) 109 it is stored in memory until the Content SC is downloaded. 147 The End-User Device(s) 109 request from the Content Hosting Facility 111, sending the corresponding License SC for the purchased Content 113. 148 Content 113 is sent to the End-User Device(s) 109. Upon the receipt the Content 113 is de-encrypted by the End-User Device(s) 109 using the Symmetric Key.

Detailed Description Paragraph Table (8):
BOM Key Description Part Parts Part Exists Digest Result Name Encrypt Alg Key ID/Enc Key Sym Key Alg Sym Key ID SC Version SC ID SC Type SC Publisher Date Expiration Date Digest Algorithm ID Digital Signature Alg ID Transaction ID Yes Yes Output Part RSA CH Pub Key End-User(s) ID Yes Yes Output Part RSA CH Pub Key End-User(s)' Public Key Yes Yes Offer SC(s) Yes No Offer SC(s) BOMs Yes Yes Selections of Content Use Yes Yes HTML to Display Yes Yes Key Description Part Yes Yes Electronic Digital Content Yes No Store(s) Certificate Digital Signature

Detailed Description Paragraph Table (9):
BOM Key Description Part Parts Part Exists Digest Result Name Encrypt Alg Key

ID/Enc Key Sym Key Alg Sym Key ID Metadata SC(s) Parts [Content URL] Output Part RC4 Enc Sym Key RSA CH Pub Key [Metadata URL] Output Part RC4 Enc Sym Key RSA CH Pub Key SC(s) Version SC(s) ID SC(s) Type SC(s) Publisher Date Expiration Date Clearinghouse(s) URL Digest Algorithm ID Digital Signature Alg ID Content ID Yes Yes Metadata Some Yes Usage Conditions Yes Yes SC(s) Templates Yes Yes Watermarking Instructions Yes Yes Output Part RC4 Enc Sym Key RSA CH Pub Key Key Description Part Yes Yes Clearinghouse(s) Certificate(s) Yes No Certificate(s) Yes No Digital Signature Offer SC(s) Parts SC(s) Version SC(s) ID SC(s) Type SC(s) Publisher Date Expiration Date Digest Algorithm ID Digital Signature Alg ID Metadata SC(s) BOM Yes Yes Additional and Overridden Fields Yes Yes Electronic Digital Content Yes No Store(s) Certificate Certificate(s) Yes No Digital Signature Transaction SC(s) Parts SC(s) Version SC(s) ID SC(s) Type SC(s) Publisher Date Expiration Date Digest Algorithm ID Digital Signature Alg ID Transaction ID Yes Yes Output Part RSA CH Pub Key End-User(s) ID Yes Yes Output Part RSA CH Pub Key End-User(s)' Public Key Yes Yes Offer SC(s) One Offer No SC(s) Offer SC(s) BOMs One BOM Yes Selections of Content Use Yes Yes HTML to Display in Browser Wdw Yes Yes Key Description Part Yes Yes Electronic Digital Content Yes No Store(s) Certificate Digital Signature Order SC(s) Parts SC(s) Version SC(s) ID SC(s) Type SC(s) Publisher Date Expiration Date Digest Algorithm ID Digital Signature Alg ID Offer SC(s) BOM Yes Yes Transaction SC (s) BOM Yes Yes Encrypted Credit Card Info Yes Yes Output Part RSA CH Pub Key Key Description Part Yes Yes Digital Signature

Detailed Description Paragraph Table (12):
Usage Usage Usage Condition 1 Condition 2 Condition 3 compressed encoded 384 Kbps 384 Kbs 56 Kbps version type of user private private private consumer consumer consumer type of transaction purchase rental purchase availability dates 1 Oct 1997- 1 Oct 1997- 1 Oct 1997- 31 Dec 1997 31 Dec 1997 31 Dec 1997 countries USA and USA and USA and Canada Canada Canada watermarking std. std. std. notifying events copy action none none number of copies 1 0 0 onto what media MiniDisc not applicable not applicable term of rental not applicable 14 days not applicable price Price 1 Price 2 Price 3 4. Parts of the Metadata SC(s) 620

Other Reference Publication (3):
Quantum Public Key Distribution System, IBM Technical Disclosure Bulletin, Apr. 1, 1997.*